View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by UEL Research Repository at University of East London

The digital divide in the post-Snowden era

Clark, Ian

Subject Librarian, University of East London

ABSTRACT: Edward Snowden's disclosure of mass surveillance of the internet has necessitated a re-examining of our relationship with the internet. Rather than a tool that broadens democratic engagement, the internet is increasingly used as a tool to manage and direct citizens, particularly via the mass collection of personal data by both the state and large multi-national corporations. Although online tools are available to protect intellectual privacy and ensure individuals can fully engage in the democratic process, they are subject to the same limitations as other aspects of the digital divide in terms of social, economic and cultural capital. Regarding online intellectual privacy, the evidence suggests there are more efforts by the library profession to protect the rights of the individual in the United States, the home of the NSA, than in the United Kingdom. This paper seeks to investigate the state of this aspect of the digital divide and what is being done to address it.

Keywords: mass surveillance; digital divide; intellectual privacy; democracy; libraries

This is an Open Access article distributed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Radical Librarianship, Vol. 2 (2016) pp.1–32

Introduction

In late 2012/early 2013, Edward Snowden, a contractor working for the National Security Agency (NSA), approached two journalists with information about a programme of mass surveillance conducted by the US government (Carmon, 2013). The NSA's security operations were designed to collect vast amounts of data regarding the internet use of everyone online. Furthermore, the revelations of surveillance operations suggested a relationship between the state and large corporations (MacAskill, 2013).

His realisation of the extent of the surveillance of the American population (and beyond) prompted Snowden to approach Laura Poitras and Glenn Greenwald with information about the programmes being conducted (Maass, 2013). These revelations have forced us to confront the reality of the internet. Despite the technology's potential to broaden engagement in the democratic process, it has been increasingly utilised as a tool to manage and direct populations (Lyon, 2015). State and commercial surveillance has grown to such an extent, that its operation is comparable to that adopted by totalitarian states (Giroux, 2015). Rather than strengthening democracy, increased access to the internet has instead resulted in the ascendency of surveillance infrastructures which are ultimately incompatible with liberal democratic systems of governance (Cohen, 2013). As a profession that has developed many of the "norms of intellectual freedom and privacy" (Richards, 2008), librarianship should be concerned about a programme of mass surveillance that threatens intellectual freedom and privacy (the freedom to read, think and speak).

Since the emergence of the internet, librarians have been concerned with the consequences of the "digital divide" – the gap between those with meaningful access to the internet, and those without (DiMaggio & Hargittai, 2001). But the "digital divide" should not be considered purely in terms of access, it also needs to be understood in terms of skills – the divide between those who can exploit the internet to their advantage, and those that cannot. In the post-Snowden digital landscape there is an additional element to this skills divide to consider – the divide between those who can navigate the internet free from state and corporate oversight, and those who cannot. Although there have been studies in the United States on the ability of different social groups to protect themselves from unwarranted online surveillance (Park, 2013), there has been little significant analysis of online privacy and the digital divide in the United Kingdom. Indeed, the study of digital inclusion has rarely factored in issues related to surveillance and privacy (Gangadharan, 2012).

This paper explores the implications of privacy and surveillance technologies regarding digital inclusion in the UK. It examines online surveillance, the usability of encryption tools designed to protect intellectual privacy online, the state of the digital divide, and the role of library and information professionals in this area.

The digital divide

Initial conceptions of the digital divide primarily focused on access to the internet, particularly in terms of whether an individual did or did not go online (Hargittai, 2002). As access has grown, so has focus shifted away from whether or not an individual has access to an internet connection and towards how they actually use it (Hargittai, 2002; Park, 2014; Sparks, 2013). In particular, there has been growing interest in the impact of the internet on the "political behaviour of citizens" (De Marco, Robles, & Antino, 2014). Despite growing access to the internet, the evidence suggests that rather than broader engagement, political discourse continues to be dominated by elite groups with the digital skills divide exacerbating the democratic deficit (Hargittai, 2002; Mervyn, Simon, & Allen, 2014; Min, 2010; Sparks, 2013).

DiMaggio and Hargittai (2001) identified five key dimensions along which such a divide might exist: technical means (hardware and connections), social support networks available to users, skill in using the internet, their purposes in using the technology, and autonomy of use (whether use is monitored or unmonitored). As Gangadharan (2012) observed before Edward Snowden disclosed the activities of the NSA, the study of digital inclusion with regards to privacy and surveillance has received little attention. In the light of Snowden's disclosures therefore, it is increasingly important to consider the impact of surveillance upon those connected to the internet and, in particular, to examine the extent to which citizens can exhibit autonomy in their use of it as a consequence of these conditions.

In terms of digital inclusion more generally, Fuchs (2010) observes that people with high income, good education, and high skills are more likely to have access to the internet and to be highly capable using it compared to those endowed with very little economic (ability to purchase equipment), social (a networking of skilled support and contacts), or cultural capital (ability to invest time to improve skills). All such manifestations of capital are fundamental factors in the extent to which people are able to ensure autonomy of internet use. There is a need to purchase the equipment that offers the best security, the need to invest time to develop skills to use encryption technologies effectively and access to a network of skilled, knowledgeable contacts to ensure guidance on using the technology effectively. Before exploring the skills and knowledge required to ensure privacy and enable citizens to exhibit autonomy in their use of the internet, we must understand how surveillance operates and the conditions of the surveillance society that we inhabit.

Justifying surveillance as a security strategy

State surveillance is not a recent development in terms of the management and control of individuals, however the events of September 11th 2001 led to a substantial expansion of surveillance, deepening a culture of fear and suspicion (Fuchs, 2010). Surveillance has

expanded to such an extent that although it is not ubiquitous, its presence has become normalised and is a generally accepted part of modern living (Fuchs, 2010; Giroux, 2015). Part of this extensive expansion of surveillance is a consequence of the increased use of digital communication technologies by terrorist organisations. Whereas organisations such as ETA and the IRA relied on word of mouth or the media to distribute attack warnings, terrorist groups now utilise the internet to disseminate propaganda, communicating directly with supporters and potential converts (Brown & Korff, 2009).

Proponents of surveillance as a security strategy argue that the use of public and private surveillance leads to greater security from crime and terrorism (Richards, 2013) and that its use enables European states to meet their obligation to protect their populations against possible terrorist acts (Council of Europe, 2002). In the UK, Osman v United Kingdom also reinforced this obligation, but further advised that there is an imperative to respect the guarantees contained within Articles 5 and 8 of the European Convention on Human Rights (European Court of Human Rights, 1998). Article 8 guarantees the right for the respect of an individual's private life and specifically entrenches the data protection rights of citizens (Brown & Korff, 2009). It is also subject to a robust interpretation by the European Court of Human Rights (ECHR) to ensure government surveillance is restricted (Brown, 2014). There is, therefore, a tension between the need to protect the individual from supposed external threats and the right of the individual to a private life – surveillance corrodes civil liberties, but it also manages threats (Richards, 2013).

The act of surveillance

Although there are justifications for the use of targeted surveillance, the implementation of mass surveillance raises serious concerns. Michel Foucault's interpretation of Jeremy Bentham's panopticon is often used as a starting point when seeking to understand the impact of surveillance on the individual (Lyon, 1994). Bentham proposed the design of a prison with a central tower that would enable supervisors to view all the cells at any one time without the prisoners being able to see them (Bentham, 1995). Foucault used Bentham's idea as an example of "the automatic functioning of power", arguing that surveillance is most effective when it is permanent in its effects, even if not continuous in its actions (Foucault, 1977). For Foucault, effective power must be both "visible" and "unverifiable". Those subject to surveillance must be able to see, or be conscious of, the mechanisms used to monitor them, yet also unable to determine whether they are being monitored at any one moment. Ultimately, surveillance is at its most effective when it does not require the actual exercising of power, the individual is controlled due to the awareness that they *may* be observed. It manages and controls individuals, and therefore undermines autonomy (Lynch, 2015), on the basis of *existing*, rather than by *acting*.

The concept of surveillance as a technique to both protect and influence the individual is taken up by David Lyon, a leading figure in surveillance studies, who outlined his definition of surveillance as being the "focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction" (Lyon, 2007). Surveillance is not merely concerned with observing individuals on the basis of protecting them it is also about managing and directing those that are under surveillance, undermining their autonomy. It is as much about direction as it is about protection (Lyon, 2007). This is particularly troubling with respect to mass surveillance as we are not just observing the actions and behaviours of a minority, everyone is subject to management or direction. The unchecked expansion of such surveillance structures ultimately undermines individual liberties and fundamentally threatens the notion of liberal democracy (Cohen, 2013).

Surveillance, the state, and the individual

Surveillance inhibits our ability to formulate new, alternative ideas in relation to political and social issues because the spaces available to formulate such ideas are subject to state oversight (Richards, 2013). Recent revelations have demonstrated the extent to which these safe spaces to discuss alternative ideas to the status quo have been violated with pro-democracy movements such as Occupy and others undermined by the use of state surveillance (Giroux, 2015). Richards argues that this tactic is a threat to "intellectual privacy" – the notion that "new ideas often develop best away from the intense scrutiny of public exposure" and that a guarantee of protection from surveillance or interferences is necessary to protect such freedom (Richards, 2013). Intellectual privacy is an essential form of privacy for all. It enables everyone to explore and develop new ideas, free from the gaze of state or corporate interests, enabling the contemplation and exploration of alternatives to the status quo.

Violations of an individual's intellectual privacy by the state seeking to learn what people are reading, watching, thinking, or saying are serious threats to civil liberty. This is a key and vital area for librarians to engage in, not least because the profession has arguably developed "many of the most important norms of intellectual freedom and privacy" (Richards, 2008). To develop ideas, space must be available to explore and experiment with them, to adapt them knowing that we are doing so in private. Ultimately, surveillance can undermine our freedom of thought and skew the way we think, with clear consequences for the content of our speech or writing (Richards, 2008). This understanding of surveillance as an intellectual inhibitor is not historically controversial. In 1967, for example, the Presidential Commission on Law Enforcement and Administration of Justice recognised that the fear of being monitored can have "a seriously inhibiting effect upon the willingness to voice critical and constructive ideas" (President's Commission on Law Enforcement and Administration of Justice, 1967).

Mass surveillance by the state results in the chilling effect of limiting our intellectual privacy, inhibiting our ability to seek out new ideas that conflict with the status quo and therefore inhibiting our autonomy. This freedom to seek out new ideas, critique and dissent from the status quo is an essential element of the democratic process (Bauman, 2001; Giroux, 2015). For a democracy to function effectively, privacy of communications are essential to ensure that individuals have the space afforded them to think and engage constructively in the democratic process (Richards, 2008). As the balance between our safety and our civil liberties shifts, as the barriers to authoritarian power erode, so the ability to think critically becomes a dangerous act (Giroux, 2015). The ability to develop critical perspectives on the world in private is central to a functional democratic system and efforts by the state to use surveillance as a tool of control ensure that challenges to the status quo are contained (Bauman, 2001; Cohen, 2013; Giroux, 2015). Consequently, those who aren't served by the existing system, whether marginalised by income, gender, race, sexuality, or disability, will be inhibited from effectively critiquing and challenging the system, ensuring it is more responsive to the policy preferences of those that benefit from the status quo – typically the wealthiest in society (Morris & Morris, 2013). As a result, the ability to limit unwarranted surveillance is critical in ensuring and sustaining a fully functioning democratic system (Castells, 2004).

Surveillance and capitalism

Although surveillance is traditionally viewed as a mechanism of the state, it is also important to be conscious of the growth of corporate surveillance. The two forms of surveillance may appear distinct, but the two increasingly interact with information flowing between them in a state of "liquid surveillance" (Richards, 2013). Liquid surveillance has emerged as a consequence of the gradual shift in reducing ordinary citizens to consumers and transforming them into suspects, enabling personal data to flow as if a liquid (Lyon, 2010). Corporate surveillance can no longer be seen as a separate phenomenon. Indeed, co-operation between the state and business in collecting information on those that threaten the status quo is not a recent phenomenon, particularly in the UK (Smith & Chamberlain, 2015). The data collected by corporations is not simply sold to advertisers to make profits, remaining solely within the corporate domain, but, as Snowden's disclosures revealed, it is also accessed by the state (MacAskill, 2013).

Private companies generate profits from the commodification of personal data, collecting and selling in return for using "free" services (Richards, 2013). The rapid commercialisation of the internet from 1995 onwards was crucial in consolidating the notion that information is a commodity (Lyon, 2015). Increasingly our personal data has become a commodity for large corporations to derive profit. Global capitalism is reliant on the creation and consolidation of profit for global corporations. As a result, the commodification of

information compels global corporations to rapaciously harvest data to drive up profits. Encouraging the desire to surrender personal data is, ultimately, fundamental to the growth and consolidation of many such corporations. As such, whereas the state has previously been persuaded to reject certain surveillance techniques (Price, 2013), it is hard to see corporate entities permitting a retreat from a strategy that drives profit.

Although many online services are free to use, some of the largest are funded by advertisements that are driven by user data – the more data they accrue about online activity the more effectively these adverts can be targeted (Fuchs, 2010; Richards, 2013). The use of transactional data, profile, financial status, etc., is fundamental to the marketing strategies for online businesses and is growing as more sources of personal data emerge (Evans, 2005). For example, security firm AVG sell search and browser data to advertisers in order to "make money" from its free antivirus software (Temperton, 2015a). Through use of the service, individuals receive free security software in return for their personal data being collected and sold to generate profit.

The volume of personal data has expanded principally as a result of the emergence of social media, which has opened up new methods of communication and facilitated the harvesting of personal data for large corporations. Social media platforms are increasingly tracking, surveilling, and connecting individuals to others, undermining efforts by users to maintain their privacy (Vickery, 2014). This form of surveillance is different from that conducted by the state because it appears to be consensual. Users are neither monitored covertly nor is their data extracted without their knowledge, it is given away voluntarily. Rather than a panopticon that is imposed without consent, social media users engage in a "voluntary panopticon" (Humphreys, 2011). This voluntary panopticon results in the surrendering of personal data to benefit the user, whether for discounted services or for enhancing social status (Cohen, 2013; Giroux, 2015). As part of the neoliberal drive to turn citizens into consumers, social media plays an important role in making all aspects of life visible and subject to market forces (Giroux, 2015).

However, concerns regarding the security of personal data being held by organisations were reflected in a report by Deloitte which found that 24% of people in the UK do not trust any type of organisation with their personal data (Deloitte Insight, 2014). These concerns are particularly prevalent in the young. A report by Demos (also in the UK) found that 18–25 year olds cared more about online privacy than issues such as the environment, crime, and welfare (Birdwell, Cadywould, & Reynolds, 2015). Although many are willing to trade personal data for free services, a significant proportion are concerned about online privacy and suspicious about the storage of personal data. For those that are concerned, there is clearly a need to help them act on these concerns and minimise their exposure to the collection of their personal data.

This willingness to trade personal data for free services has prompted technologists such as Christopher Soghoian, principal technologist at the American Civil Liberties Union, to argue the need for individuals to "rethink their relationship" with many corporations and understand that if they want a secure service they will need to "pay something so the company has a sustainable business model that doesn't depend on (collecting and monetizing your data)" (Bloom, 2014). The use of free online services is ultimately a threat to online privacy as the collection of personal data is fundamental to the economic model. In a capitalist society, where money is exchanged for the products of someone's labour, the façade of a product accessible at no cost to the user may be difficult to overcome.

State and corporate collaboration

The data that is collected by communications companies in return for services does not always stay securely in their possession. In the United States, for example, records collected by corporations can be obtained by the government through a variety of means, including grand jury subpoenas or through National Security Letters (NSLs) that enable the FBI to obtain information from telephone companies, ISPs, etc. (McLaughlin, 2015; Richards, 2013). The extent of the blurring between state and corporate communications is such that concerns about the collection of personal data have led to legal actions, such as that launched by the Belgian privacy commission against Facebook for allegedly conducting surveillance comparable to the NSA (Gibbs, 2015a). Increasingly, corporate data collection is effectively state surveillance by proxy as data flows between the two in a process of "liquid surveillance". Consequently, services such as Facebook have become "a major clearinghouse for serious and systematic surveillance by corporations, crime control agencies and...security concerns" (Lyon, 2010).

The relationship between corporations and the state has strengthened with respect to surveillance and data gathering. The Department of Homeland Security, for example, was influenced by "Customer Relationship Management" (CRM) as part of the drive towards "Total Information Awareness" (Lyon, 2015). New technologies to expand surveillance have also been developed by the corporations and sold to the government, including facial recognition software developed by The Disney Corporation and sold to the US military (Wolf, 2012). The depth of this relationship is further demonstrated by the Pentagon's appointment of the CEO of Google's parent company to lead its Defense Innovation Advisory Board, which will influence "product development … [and] data analysis" (Shalal, 2016). Clearly, government and corporations are increasingly connecting, sharing information and facilitating the development of surveillance technologies such that it is creating a "brand-new domain of the state-corporate complex" (Schell, 2013) which has led to the further development of a surveillance culture (Lyon, 2015). State and corporate

apparatuses have, effectively, colluded to induct everyone into a regime of both security and commodification (Giroux, 2015).

The emergence of digital surveillance

Variations of the practices uncovered by Snowden are well established techniques practised both by the state and corporate sectors, not just in terms of state surveillance, but also in terms of consumer marketing (Lyon, 2015). Throughout the 1980s, researchers were interested in both state surveillance in relation to national security, and in terms of consumer surveillance – the latter only seriously considered as surveillance in the 1990s (Lyon, 2015). Even during this period, before mass adoption of the internet, the impact that computerisation would have on these forms of surveillance had been identified and understood (Lyon, 2015).

Surveillance strategies have historically been a fundamental strategy of the state to manage their populations, undermining autonomy. Under the pretext of national security concerns, the state has consistently violated civil liberties through the use of surveillance. From the counter-terrorism programme developed by J. Edgar Hoover in the 1950s that remained in place until the 1970s (Giroux, 2015), to the surveillance conducted by the US Army following the assassination of Martin Luther King Jr (Richards, 2013), the strategy is not a new one. As recently as the 1990s, the ECHELON system enabled the Five Eyes (the intelligence sharing partnership between the US, UK, Canada, Australia, and New Zealand) to intercept all satellite communications, allowing access to cable and radio communications worldwide (Jordan, 2015).

Surveillance has often been used as a strategy to contain the poorest and the most marginalised members of society, particularly on the basis of the suppression of working people's resistance and the containment of "alleged social contagion" (Eubanks, 2011). This was demonstrated in the United Kingdom where, at the beginning of the 20th century, agents of the state covertly photographed members of the suffragette movement on the basis that the movement presented a serious "threat to the British Empire" (Casciani, 2003; Smith & Chamberlain, 2015). This use of surveillance to contain and suppress a marginalised group campaigning for equal rights in British society demonstrated the extent to which the government was prepared to defend the status quo, limiting engagement in the democratic process. For the security services, there is an unambiguous desire to monitor those who wish to "prevent something happening or to change legislation to domestic policy" (Evans & Lewis, 2013).

Digital surveillance in the United Kingdom

The UK government has remained one of the leading proponents of surveillance, to the

extent that the United Kingdom is considered one of the most surveilled democratic states (Richards, 2013). In 2008 the UK government launched a mass digital surveillance programme (code-named KARMA POLICE) without public debate or scrutiny. The goal of the program was to record the browsing habits of "every visible user on the internet" (Gallagher, 2015). The data collected included access to news websites, social media, search engines, and chat forums amongst others, violating the intellectual privacy of those unable to protect themselves. This was followed in 2013 by The Guardian's revelations about GCHQ's Tempora program. As a result of the placement of data interceptors on cables carrying data between Europe and America, the Tempora program allowed the agency to analyse communications, including the content of email messages, Facebook posts and recordings of phone calls (Jordan, 2015; MacAskill et al., 2013). Such activities raise serious concerns for librarianship as a profession concerned with intellectual freedom and privacy: particularly in terms of how we can protect the privacy of our users and ensure their autonomy when accessing the internet, particularly in the UK.

Furthermore, both the UK and the US have been at odds with European institutions regarding the collection and use of personal data. The Safe Harbour agreement, for example, permits the safe transfer of personal data to the US without being misused in line with European Data Protection law, however this has not insulated the data from acquisition by the NSA (Bernal, 2015; European Court of Justice, 2015; McGarr, 2015; Peers, 2015). A judgement by the European Court of Human Rights (ECHR) regarding the storage of data relating to the private life of an individual has repeatedly been contested by the UK, arguing that *use* rather than *collection* contravenes Article 8 (Brown, 2011; European Court of Human Rights, 2000). Despite the UK's protests, the European Court has comprehensively rejected the view that the collection of data does not affect privacy rights (European Court of Human Rights, 2008).

Despite concerns across Europe, however, the UK remains relatively aggressive in its use of surveillance technologies, regardless of rulings by the ECHR. In 2015, for example, the Investigatory Powers Tribunal (IPT) revealed that GCHQ (Government Communications Headquarters) had spied on two international human rights organisations and confirmed that the "Wilson Doctrine" (an agreement that protects parliamentarians from surveillance and therefore ensures confidentiality between elected representatives and the people they represent) was not "legally enforceable" (The Investigatory Powers Tribunal, 2015a, 2015b). Furthermore, the IPT also ruled that it is legal for GCHQ to hack into systems in the UK and overseas to install spyware (Moody, 2016; The Investigatory Powers Tribunal, 2016) and the UK government has also sought to be able to serve wiretap notices on communications firms in the United States with regards to the activities of British citizens (Moody, 2016; Nakashima & Peterson, 2016).

The UK government has also repeatedly attempted to pass a Draft Communications Data Bill (or "Snoopers Charter") into law (Home Office, 2012) to monitor online communications. The Bill intended to compel technology and telecoms companies to collect and store metadata for up to a year and make it available to authorities without a warrant (Temperton, 2015b). These proposals have subsequently been revised and renamed as the Investigatory Powers Bill (Home Office, 2016b). The bill proposes that internet connection records (ICRs) must be retained by the communication service providers (CSPs) "when served with a notice requiring them to", in effect ensuring access to a record of the "services that they have connected to" (Home Office, 2015, 2016b). This has clear implications for library services (including public and academic libraries) and the profession in general as the draft legislation would require libraries to store internet usage data and pass to the state as required, threatening the autonomy of our users (Travis, 2016). The bill itself has been criticised by the United Nations' Special Rapporteur on the right to privacy (Cannataci, 2016) and it is not clear at present to what extent the ECHR ruling in the case of Zakharov v Russia outlawing mass surveillance will impact its progress into law (European Court of Human Rights, 2015; St Vincent, 2016).

Encryption technologies are vital in protecting intellectual privacy and ensuring autonomy of internet use, one of the five forms of digital inequality identified by DiMaggio and Hargittai (2001). They can also play a key role in protecting the reading habits of library users. However, the UK government appears hostile to encryption, with Prime Minister David Cameron arguing that the government should not "allow a means of communication between people which ... we cannot read" (Mason, 2015). As a result of this, it has been suggested that the government may seek to secure backdoors to encrypted services (Temperton, 2015c), undermining the intellectual privacy of all internet users. The Investigatory Powers Bill currently under consideration includes an obligation upon CSPs to "remove any encryption applied by the CSP to whom the notice relates" (Home Office, 2016a). Furthermore, the legislation indicates that such an obligation will only apply to "electronic protections that have been applied by, or on behalf of, the company on whom the obligation has been placed" (Home Office, 2016a). As some companies in the technology industry move towards strong encryption (or "electronic protections") that they themselves cannot break and therefore do not control (Bernal, 2016), this raises questions about the extent to which encryption technologies are vulnerable to such demands by the Home Office. However, the British public, who largely oppose the operations conducted by the NSA (Pew Research Center, 2014), do not share this hostility – 43% oppose a "ban" on "encryption software" (YouGov, 2015).

Despite concerns about the extent to which encryption technologies are utilised by terrorists to evade intelligence agencies, the use of such technologies appears to be no more common amongst terrorists than the general population (Brown & Korff, 2009). Although the CIA

have raised concerns regarding the use of encryption technologies following Snowden's disclosures (Brennan et al., 2015), a 2014 report by Flashpoint found that there had been little evidence to suggest that jihadist groups were increasingly using the technology (Flashpoint Partners, 2014). Furthermore, a report by Harvard's Berkman Center for Internet and Society questioned the extent to which encryption impedes intelligence gathering on criminal activity and underlined the importance for corporations of being able to monetise data, noting that the technology is unlikely to be "adopted ubiquitously by companies, because the majority of businesses … rely on access to user data for revenue" (Olsen et al., 2016).

Whilst the government threatens to eliminate encrypted communications, its availability enables those that have the skills and knowledge to defend their intellectual privacy in the face of a government hostile to such a principle. For those that lack skills and knowledge however, there is a clear threat to their intellectual privacy, exposing them to risk of greater surveillance and, consequently, limiting their ability to engage fully in the democratic process. As DiMaggio and Hargittai observe, autonomy of use of the internet must be considered a key component of the digital divide (DiMaggio & Hargittai, 2001). Without the freedom that encryption technologies provide in an environment of mass surveillance (Reiman, 1996; Rogaway, 2015), one clearly cannot exercise such autonomy. As the United Nations Special Rapporteur on freedom of expression concluded in their 2015 report, "encryption and anonymity enable individuals to exercise their rights to freedom of opinion and expression in the digital age" (Kaye, 2015). Library and information workers must, therefore, consider the lack of skills to protect online intellectual privacy as a key aspect of the digital divide and, as a profession, seek ways to overcome this aspect of digital inequality.

Protecting intellectual privacy through encryption

Given the effects of mass surveillance, being able to defend individual intellectual privacy and ensure autonomy with respect to internet usage is crucial in ensuring information can be accessed freely and citizens are able to seek out ideas that challenge the status quo. If only certain sections of society are able to protect their intellectual privacy online, to seek out ideas that challenge the status quo, the democratic potential of the internet will be seriously undermined (Min, 2010). Without the ability to freely seek out ideas that challenge the status quo, to organise and resist, then clearly the status quo will prevail. Access to online tools that ensure the protection of intellectual privacy are therefore crucial for tackling this aspect of digital inequality, enabling the potential for broader democratic engagement.

Online tools that provide end-to-end (E2E) encryption are vital in ensuring freedom of speech and the protection of intellectual privacy (Reiman, 1996; Rogaway, 2015; Vagle,

2015). Although encryption does not typically protect metadata (email addresses, mobile phone location data), it does protect the content of what is encrypted (Cox, 2016; grugq, 2015b; Olsen et al., 2016). Post-Snowden, there has been growing interest in the use of such tools and a growing number of tools that seek to take advantage of concerns regarding surveillance. There has, for example, been a growth in instant messaging apps that offer encrypted communications, such as Telegram, Whatsapp, and Signal (formerly TextSecure) (Dredge, 2014). Although there has been growth in instant messaging tools that facilitate encrypted communications, Snowden's disclosures haven't had a comparable impact on other encryption tools such as PGP email encryption technologies (Renaud et al., 2014).

Given the supposed role of the library profession in developing the norms of intellectual privacy, the ability to seek information online without fear of being observed must be considered crucial in protecting intellectual privacy and enabling autonomy of internet use. In an environment of mass surveillance of web activity (by both the state and corporations) the protection of such activity is fundamental in ensuring intellectual privacy. One of the most popular tools to protect web activity is Tor Browser. Tor passes web traffic through a series of nodes to obfuscate its source and Tor Browser is considered an effective tool to ensure anonymity when accessing the internet (Norcie et al., 2014; Schriner, 2015). Due to the nature of its operation, it is impossible to precisely determine how many people use the Tor network, but as of December 2015 there were an estimated two million "directly-connecting clients" (Tor Metrics, 2015).

Tor may be effective in preventing third parties from observing and collecting data about a user's web activity, but it is still susceptible to threats including "subversion via control of malicious nodes and timing attacks" and attempted deanonymisation of users (arma, 2014; Norcie et al., 2014). As with all online tools, the Tor network has its vulnerabilities and it is important to be clear of its limitations as well as acknowledging that it offers significantly greater protection than the more commonly used tools that currently exist. However, the biggest issue for Tor is the amount of users utilising the software – the more that use it, the more effective it becomes, further increasing the anonymity of its users (Norcie et al., 2014). Fundamental to increased security through anonymity, therefore, is ensuring that online anonymity tools are easily usable, enabling more to use it effectively and consequently improve the privacy of the entire network as well as ensuring wider defence of intellectual privacy (Norcie et al., 2014).

In terms of the usability of security software, a different standard of usability needs to be applied in comparison to standard software (Whitten & Tygar, 1999). In order for the software to be used effectively, it is vital to ensure that those who are expected to use it:

- Are reliably made aware of the security tasks they need to perform.

- Are able to figure out how to successfully perform those tasks.
- Don't make dangerous errors.
- Are sufficiently comfortable with the interface to continue using it (Whitten & Tygar, 1999).

If users experience difficulties with any of these elements, individuals will not be able to use the software effectively, putting themselves at risk. Ultimately, the lack of usability could result in "censorship, surveillance and...physical harm" (Norcie et al., 2014).

Regarding the usability of Tor Browser, Norcie et al. (2014) found that, in the first of the two groups they studied, significant numbers of students experienced difficulties, even though they were "more educated, more familiar with computer security, and more male than the general population". Although the second study group saw a significant improvement in usability (after improvements made by the Tor Project), issues were still evident (although on a smaller scale) despite their familiarity with computer security.

A further study by Renaud et al. (2014) on E2E email encryption identified seven fundamental states in terms of encryption and privacy enhancing tools:

- Lack of awareness of privacy as a concern.
- Awareness of possibility of privacy violation but don't take action, maybe due to lack of concern.
- Aware of possible violation but not aware this can happen in transit or at the mail server side. They attempt to protect themselves, but not using E2E encryption.
- Aware but not see the need to act.
- They are aware of potential violations and wish to act, but they do not know how.
- They are concerned about privacy and understand E2E encryption prevents this, but they can't do it.
- They are concerned and understand they can use E2E but they still have reasons not to (may get side-tracked or other reasons).

They found that "very few" of the participants mentioned the term encryption and many of those that did "seemed to have a wrong understanding of encryption and in particular E2E encryption". There is, clearly, a lack of awareness of the technology, what it achieves and how it operates, which may lead to difficulties in distinguishing tools that provide strong protections from "snake-oil alternatives" which may leave them vulnerable (Sinclair Brody, 2016). They also concluded that although usability may be an issue, this would only be the case for those who reach the stage of wishing to act. For many, privacy may be considered

secondary to the function individuals wish to perform (Sinclair Brody, 2016). For those who do not adopt such technologies, it is first necessary to overcome their lack of will or ability to protect their intellectual privacy. For those that do reach the stage of using it, however, it is clear that E2E email encryption is "undeniably effortful" and harder to use than normal software (Renaud et al., 2014; Sinclair Brody, 2016; Whitten & Tygar, 1999).

Other tools to enable secure communications have also proved problematic. For example, Mailvelope, a PGP email client, was found to be difficult to use by the majority of participants in one study, with almost all participants unable to complete the required tasks (Ruoti et al., 2015). As a result of the study, Ruoti et al. argued that it is "unclear if PGP will ever be usable by the masses" concluding that "Johnny has still not gotten any closer to encrypt his email using PGP" (Ruoti et al., 2015). Furthermore, the use of IM protocols such as XMPP (formerly Jabber), in combination with Off-the-Record (OTR) encryption protocols to ensure end-to-end encryption, can be particularly arduous with a number of steps required before secure communications can be conducted (Lee, 2015a).

Although there are limitations in drawing out substantive conclusions from such studies, it is clear that as those who are described as "more educated" and "more familiar with computer security" experience difficulties, one can conclude that those who aren't as educated or as familiar with computer security are as likely to experience difficulties, if not more so. Further research is, of course, needed to establish the extent to which the general population experience difficulties using technologies that protect their intellectual privacy. Furthermore, although those who are "computer savvy" may be familiar with privacy enhancing tools such as Tor, it is unclear to what extent the average member of the public is either aware of the technology or understands its value. As Renaud et al.'s study found, few of those that participated even mentioned encryption so one can reasonably expect that this lack of understanding of encryption technologies is fairly widespread, if not within the "computer savvy" community, then certainly across society generally.

As well as skills, the ability to identify which tools are most effective at protecting the user is also fundamental. Not all tools that claim to provide secure messaging provide a truly secure communications platform. Although there has been a proliferation of instant messaging tools offering encrypted communications, it is arguable that many services ultimately seek to profit from growing concerns about state and corporate surveillance. Telegram, for example, despite running a competition encouraging individuals to test its encryption (Telegram, 2014), has been decried as "error prone" and "leak[ing] voluminous metadata" (Cox, 2015; grugq, 2015a). In contrast, Signal (an open-source messaging tool) provides the "best encryption available" (grugq, 2015b). The ability to recognise which tools are most effective, as well as having the skills to use encryption tools effectively, is fundamental to ensuring the

protection of intellectual privacy. It is, therefore, crucial for individuals to be aware of the appropriate tools to protect their intellectual privacy.

Furthermore, access to suitable hardware must also be considered. In one study comparing the two most popular operating systems in mobile devices (iOS and Android), it was found that iOS devices had a slight advantage over Android devices in terms of security (Ahmad et al., 2013). This is significant because devices running on the Android operating system tend to be cheaper than those running iOS (Price, 2015). Additionally, despite the enabling of encryption on the latest versions of both operating systems, the majority of Android users own devices that pre-date its adoption (Cunningham, 2015; Gibbs, 2015b). As Christopher Soghoian argues, Android devices may be relatively cheap, but they are also an easier target for intelligence agencies because they are less secure (Simonite, 2015). As a consequence, Soghoian argues that we "now find ourselves in not just a digital divide but a digital security divide", not least because Google "gives away services for free in return for access to data" (Simonite, 2015). As with other aspects of the digital divide, financial limitations and lack of skills exacerbate the post-Snowden intellectual privacy divide, limiting autonomy in our communications.

Although iOS devices are arguably more secure than their Android counterparts, they are not without their vulnerabilities. Intelligence agencies have, for example, been successful in infiltrating computers that individuals use to sync with their iOS devices (Zdziarski, 2014). Despite this limitation it is clear that, although there are vulnerabilities with both devices, iOS devices offer more security than their cheaper counterparts. This raises significant issues as those who can afford to protect themselves are able to do so by investing in more expensive hardware. Those who cannot afford it are left with devices that are inferior in security terms and, consequently, more susceptible to state surveillance.

The state of the digital divide in the UK

The most recent 'Internet Access – Households and Individuals' report by the Office for National Statistics (ONS) reflects the current state of the digital divide (ONS, 2015). The report reveals that only 35% of those surveyed have changed their internet browsing settings to prevent or limit cookies, despite 65% being aware that such cookies "can be used to trace movements of people, make a profile of each user and provide tailored ads". The ONS also found that of those households without internet access (14%), 31% reported that the reason for a lack of access was due to a "lack of skills", 14% indicated prohibitive equipment costs, and 12% access costs (ONS, 2015).

Alongside the ONS report, Ofcom found that 64% of internet users use the same password for most or all websites, 26% do not read privacy statements at all (43% say they "skim-read"), and 68% say that they are happy to provide personal information online "as long as

they get what they want" (Ofcom, 2015). Meanwhile, in a report published in 2014, the BBC claimed that 1 in 5 adults lacked four basic online skills (send and receive emails, use a search engine, browse the internet, and fill out an online application form) (BBC Learning, 2014).[1] This was particularly stark amongst the most disadvantaged as 69% of those that lacked the basic skills defined were from C2DE households.[2]

It is important to note, however, that the use of encryption technologies was problematic even for those described as "computer savvy". Consequently, although it is vital to acknowledge that the most disadvantaged will be least likely to protect themselves (which is particularly crucial as this is the group most likely to be affected by surveillance technologies), lack of skills in using encryption technologies is not restricted only to those households identified as C2DE. The intellectual privacy divide cuts across all social groupings to varying degrees, but the consequences of this divide will be felt most starkly by those that are most disadvantaged.

Libraries and the intellectual privacy divide

Libraries have been fundamental in bridging the digital divide for the most disadvantaged in society, both in providing access and in supporting the development of basic skills. The People's Network, for example, was a key government initiative that ensured public libraries played a central role in bridging the digital divide, facilitating access to the internet through the provision of accessible computer terminals available to the public (Big Lottery Fund, 2004). A related initiative to provide staff training was "fundamental to the implementation" of the People's Network – an acknowledgement that the provision of an internet connected terminal was insufficient without skilled support (King et al., 2006).

As part of the rollout of this initiative, the New Opportunities Fund (NOF) financed an information communications technology (ICT) training programme for public library staff (Library and Information Commission, cited in Spacey, 2003). The training stipulated a number of outcomes including competence with ICT and using ICT to find information for users (Spacey, 2003). Spacey found that the majority of respondents were positive about helping the public use the internet. Around 51.5% of respondents claimed they felt "generally positive" about doing so, compared to 5.4% who felt generally negative and 2.6% who felt very negative. Spacey concludes that the NOF training helped to familiarise staff with ICT and provide them with the skills for effective use of the internet, particularly those

1 A further report in 2015 was prepared by Ipsos MORI on behalf of Go ON UK that changed the four basic skills to five: managing information, communicating, transacting, creating and problem solving (Ipsos MORI, 2015). As the earlier report is more specific in terms of what it is measuring, that is the report that has been used here. In terms of the more recent report, Ipsos MORI found that 35% of C2DEs lack basic digital skills and 30% lack basic online skills.
2 C2: Skilled manual occupations, D: semi-skilled and unskilled manual occupations, E: casual workers, non-working and pensioners

with little or no ICT skills. However, no such training on online privacy was built into this package of training for library staff.

Since the roll out of the People's Network, public libraries in the UK have been in steady decline with many closed or handed to volunteers to run. As a result, the support available for basic internet skills has been greatly diminished, with some volunteer-run libraries not able to provide the skilled support required, particularly in areas of high deprivation (Clark, 2012). Consequently, public libraries have gradually been superseded as places to seek out support with the skills that are required to perform basic tasks online. Increasingly, private companies have stepped in to provide the support with online skills, effectively privatising the People's Network.

The Barclays Digital Eagles scheme, for example, offers a range of sessions designed to help people build their confidence using computers and the internet (Barclays, 2015). The support offered includes help with email, internet search engines, and online shopping. Although they offer some basic privacy advice ("beware of scam emails") the series of guides produced by Barclays offer no guidance regarding privacy protection tools available online (Barclays, 2015). The main services recommended by Barclays include Google (for search and email), Yahoo!, and Outlook.com – all of which have been either forced to hand over data to, or have had a relationship with, the NSA (Greenwald et al., 2013; Leopold, 2014; Rushe, 2014). Additionally, Google uses browser history to serve adverts to Gmail accounts, potentially leading to Barclays adverts being delivered direct to the user following such a session (Clark, 2016; Google, 2015).

As well as helping to bridge the digital divide, public libraries have a fundamental role to play in terms of intellectual privacy. In 2005, the Chartered Institute for Library and Information Professionals (Cilip) produced a "Statement on intellectual freedom, access to information and censorship" (Cilip, 2005). Furthermore Cilip endorsed the Council of Europe's 'Public access to and freedom of expression in networked information: Guidelines for a European cultural policy' (Council of Europe, 2000). Cilip's statement on intellectual freedom underlined Cilip's ethical principles that professionals must show a "commitment to the defence, and the advancement, of access to information, ideas and works of the imagination" (Cilip, 2012). The Council of Europe's guidelines put forward a number of proposals advising that individuals are to "decide for themselves what they should, or should not, access" and that those providing the service should "respect the privacy of users and treat knowledge of what they have accessed or wish to access as confidential" (Council of Europe, 2000). Librarians should, therefore, do what is required to ensure that privacy of users is respected and treat their activities as confidential. In an environment of mass surveillance it is incumbent on librarians to take steps to protect the privacy of their users.

Further to these principles outlined by the Council of Europe and endorsed by Cilip, the

International Federation of Library Associations and Institutions (Ifla) issued a statement in 2015 reinforcing the importance of libraries as places that should ensure the privacy and freedom of individuals accessing information. Ifla's 'Statement on Privacy in the Library Environment' made a number of recommendations including advising information professionals that they have a responsibility to "reject electronic surveillance", provide training on "tools to use to protect their privacy" and "respect and advance privacy at the level of practices and as a principle" (Ifla, 2015). In terms of the guidance produced by Cilip, the Council of Europe, and Ifla, librarians in the UK have an obligation to defend the intellectual privacy of those that use the services they provide.

Librarians in the US have been at the forefront in defending the intellectual privacy of library users, establishing many of the fundamentals of intellectual freedom and privacy (Richards, 2008). For example, the American Library Association's (ALA) Bill of Rights, first adopted in 1939, asserts that libraries should "cooperate with all persons and groups concerned with resisting abridgment of free expression and free access to ideas" (ALA, 1996). Furthermore, after 9/11, the ALA published an interpretation of the Bill of Rights arguing that libraries must preserve the "right to open enquiry without having the subject of one's interest examined or scrutinised by others" and that rights to privacy are "necessary for intellectual freedom and are fundamental to the ethics and practice of librarianship" (American Library Association, 2002).

Librarians tackling digital surveillance

Following the Snowden revelations in 2013, Alison Macrina established the Library Freedom Project in the US and began to visit public libraries across the country providing "privacy rights training", particularly focusing on encryption technologies (Burns, 2015; Carpenter, 2015). In 2015, the Library Freedom Project established a Tor relay node in Kilton Library, New Hampshire (Macrina & Fatemi, 2015), the first such relay in a public library anywhere in the world. Tor relays essentially act as nodes "pass[ing] traffic between each other to make the three layers of anonymizing encryption possible", and are crucial to the effectiveness of the service (Macrina, 2015). Despite efforts by Homeland Security leading to the suspension of the programme, the relay was eventually re-established (Doyle-Burr, 2015; Dreyfuss, 2015). Furthermore, legislation has been proposed that would permit libraries to install and use cryptographic privacy software, including Tor (O'Neill, 2016). The establishment of a Tor relay in a public library in the US demonstrates that it is possible to ensure the privacy of library users in an environment of mass state surveillance, ensuring greater autonomy in their use of the internet.

In the US there have been increasing efforts to raise awareness of intellectual privacy issues. For example, the ALA announced sponsorship of "Let's Encrypt", a service provided by the

Internet Security Research Group (ISRG) that enables those who own a domain to obtain an SSL certificate for a web server at no cost, ensuring protection of web traffic (ALA Office for Intellectual Freedom, 2015). Furthermore, the Electronic Frontier Foundation (EFF) submitted an amicus brief representing groups such as the ALA challenging the NSA's programme of mass surveillance in an effort to recognise the right to privacy of an individual's reading choices (Crocker et al., 2015; Crocker, 2015).

One significant advantage in tackling violations of intellectual privacy in the United States is the US Constitution, in particular the rights guaranteed under the First Amendment. These constitutional rights provide a lever which librarians can use against the state to defend intellectual privacy. Such a lever has been successfully employed previously in the case of four Connecticut-based librarians who objected to the National Security Letter provision of the Patriot Act that enabled the FBI to demand patron library records (Lichtblau, 2005). The four librarians successfully faced down the US government after refusing to turn over the requested records (Dobija, 2014). In contrast, the United Kingdom has no written constitution (and no equivalent to the First Amendment), and therefore an equivalent lever does not exist for library and information professionals. As a result, actions to defend civil liberties in opposition to the state are substantially more difficult.

Furthermore, although public libraries in the United States receive federal funding, the federal government does not "superintend" the service to the same extent as the UK government (ALA, 2015). In the UK, the government has a duty to oversee the public library service and, where a local authority fails to perform its duties, the Minister for the Department for Culture, Media and Sport has the power to intervene (Cilip, 2013). Such an intervention has a precedent following the decision to intervene in the proposals to close eleven libraries in the Wirral (Charteris, 2009; Harris, 2009). With such oversight from a government hostile to encryption technologies, it is hard to see how extensive efforts could be taken to teach the skills required for users to ensure their intellectual privacy through tools such as PGP and Tor Browser.

However, although the introduction of certain services and training on encryption technologies appears unlikely given the oversight by central government, there are non-controversial tools that could be used and advocated in public libraries to protect intellectual privacy. For example, privacy orientated search engines such as DuckDuckGo rather than Google could be adopted as default search engines ensuring personal data is neither stored nor monetised (Farivar, 2012). Library websites (particularly the library catalogue) should utilise the HTTPS protocol by default to encrypt and protect traffic between the browser and the server, protecting intellectual privacy when searching the catalogue and ensuring confidentiality (Shema, 2011). The use of open-source alternatives to proprietary software would also be advantageous, particularly as such software can better protect privacy (Barron,

2016; Sinclair Brody, 2016). Furthermore, defaulting to the use of open-source browsers such as Firefox and incorporating ad-blockers would help to remove vulnerabilities that can compromise user privacy (Lee, 2015b). A case for such measures to be taken in public libraries can and should be made as a first step towards ensuring the intellectual privacy of library users.

At present, in contrast to the efforts of library associations and librarians in the US, UK equivalents to the Library Freedom Project have not emerged and there are currently no efforts by Cilip comparable to those of the ALA. At present there are no training programmes for the general public to ensure the protection of intellectual privacy, despite Ifla's recommendations (Ifla, 2015). However, there are groups emerging in the UK that do provide such training programmes (Brass Horn Communications, 2015). Despite this, in the current environment the delivery of such programmes in public libraries managed by local authorities seems unlikely. In terms of intellectual privacy, it appears at present that there are more efforts to protect the rights of the individual in the home of the NSA than there are in the UK.

Conclusion

This paper has investigated some of the key issues concerning digital surveillance in the UK, how its existence threatens civil liberties and intellectual freedom, and the ways in which individuals can protect themselves from state and corporate infringement of these values identifying the need to provide support to develop the skills necessary to do so. Recommendations are made relating to the role of public libraries in addressing this aspect of the digital divide and supporting citizens in resisting mass state and corporate surveillance.

Mass digital surveillance is a threat to intellectual privacy, autonomy of web use, and democracy itself. Its existence inhibits the formation of new ideas and the seeking out of alternatives to the status quo, limiting the ability to critique institutions and to develop and enhance democratic structures. The state may argue that it is necessary to protect individuals from external threats, but it is also a means to maintain the status quo. Furthermore, corporate actors collect vast volumes of personal data that are then sold to create profit, a natural consequence of the commodification of information. These two forms of surveillance are not distinct: they feed into each other, with corporate surveillance acting as state surveillance by proxy.

The emergence of tools to protect individuals from mass state and corporate surveillance is crucial in ensuring citizens are able to exercise autonomy in internet use. However, these tools require the individual to have a degree of social, economic, and cultural capital. The user must be able to use and identify the right tools to ensure their intellectual privacy. Given

that many of the most disadvantaged in the UK lack basic online skills, it is clear that inequality in terms of autonomy of internet use is a serious concern in terms of digital inclusion, particularly as the UK government continues to aggressively pursue further surveillance powers.

In the US, there are ongoing efforts to ensure that individuals' intellectual privacy is protected. Despite the aggressive pursuit of surveillance powers by the UK government, there are currently no such efforts in the UK to provide individuals with the tools to access information online freely and without fear of reprisals. This inaction is at odds with the stated principles of organisations such as Ifla and Cipfa who endorse the right for individuals to access information online confidentially. At present, this is not possible in the UK as the public library network does not ensure the privacy of those who use it, thus inhibiting intellectual privacy. The situation is exacerbated by the outsourcing of digital skills support to companies with a vested interest in not introducing individuals to encryption technologies because it will inhibit the companies' ability to generate profit.

However, there are feasible actions that could be taken now. Defaulting to privacy enhancing search engines such as DuckDuckGo would ensure the protection of the intellectual privacy of users, as would the incorporation of the HTTPS protocol on websites and the use of ad-blockers on browsers. However, these are only first steps towards protecting the intellectual privacy of users. Efforts are already taking place in the UK to provide training on online privacy tools such as Tor Browser (Brass Horn Communications, 2015). Librarians should investigate the possibilities to work with such organisations to protect users, either within the context of their working environment, or as professionals seeking to ensure the privacy of individuals more broadly. Consequently, librarians should commit to familiarising themselves with existing privacy enabling tools to ensure they can advocate for them and provide support in their use. They should also seek to work with open-source developers to deliver products that provide a better user experience, helping to "professionalize the practice of open-source development" (Sinclair Brody, 2016). As various professional organisations have stated the need to ensure intellectual privacy, there is a responsibility for library and information professionals in a post-Snowden environment to take steps to tackle this aspect of digital inequality. Librarians have played a key role in tackling digital inequality and must continue to work to eradicate such inequality, ensuring autonomy of internet use and supporting citizens in protecting themselves from mass state and corporate surveillance.

References

Ahmad, M. S., Musa, N. E., Nadarajah, R., Hassan, R., & Othman, N. E. (2013). Comparison between android and iOS Operating System in terms of security. *2013 8th International Conference on Information Technology in Asia – Smart Devices Trend: Technologising Future*

Lifestyle, Proceedings of CITA 2013, 2–5. https://doi.org/10.1109/CITA.2013.6637558

ALA Office for Intellectual Freedom. (2015). ALA's Office for Intellectual Freedom announces sponsorship of Let's Encrypt initiative. Retrieved 8 November 2015, from http://www.oif.ala.org/oif/?p=5536

American Library Association. (1996). Library Bill of Rights. Retrieved 27 November 2015, from http://www.ala.org/advocacy/intfreedom/librarybill

American Library Association. (2002). Privacy: An Interpretation of the Library Bill of Rights. Retrieved 27 November 2015, from http://www.ala.org/Template.cfm?Section=interpretations&Template=/ContentManagement/ContentDisplay.cfm&ContentID=88625

American Library Association. (2015). Key Issue: Library Funding, 8410. Retrieved 11 March 2016, from http://www.ala.org/offices/sites/ala.org.offices/files/content/ogr/FINAL LIBRARY FUNDING One-Pager SJM 06-17-15.pdf

arma. (2014). Tor security advisory: "relay early" traffic confirmation attack. Retrieved 2 December 2015, from https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack

Barclays. (2015). Barclays Digital Eagles. Retrieved 15 November 2015, from http://www.barclays.co.uk/DigitalEagles/P1242671738729

Barron, S. (2016). 11 open-source alternatives. Retrieved 23 February 2016, from https://undaimonia.wordpress.com/2016/01/07/open-source-listicle/

Bauman, Z. (2001). *The individualized society*. Cambridge UK: Polity Press.

BBC Learning. (2014). *BBC Basic Online Skills*. Retrieved 11 March 2016, from http://downloads.bbc.co.uk/aboutthebbc/insidethebbc/whatwedo/learning/audienceresearch/basic-online-skills-nov-2014.pdf

Bentham, J. (1995). *The Panopticon Writings*. (M. Bozovic, Ed.). London: Verso.

Bernal, P. (2015). The Surveillance Elephant in the Room…. Retrieved 27 November 2015, from https://paulbernal.wordpress.com/2015/10/07/the-surveillance-elephant-in-the-room/

Bernal, P. (2016). You can't deny message encryption to some individuals without denying it to all. Retrieved 11 March 2016, from http://blogs.lse.ac.uk/businessreview/2016/03/08/you-cant-deny-encryption-to-some-individuals-without-denying-it-to-all

Big Lottery Fund. (2004). *The People's Network: evaluation summary*. Retrieved 11 March 2016, from http://www.biglotteryfund.org.uk/er_eval_peoples_network_evaluation_summary_uk.pdf

Birdwell, J., Cadywould, C., & Reynolds, L. (2015). Tune In, Turn Out. *Demos*. Retrieved 11 March 2016, from http://www.demos.co.uk/files/Tune_in_-_web.pdf?1419813387

Bloom, D. (2014). SXSW: Edward Snowden Panel Says Don't Count On Ad-Based Online

Companies To Safeguard Your Data. Retrieved 8 November 2015, from http://deadline.com/2014/03/edward-snowden-sxsw-panel-internet-privacy-696465/

Brass Horn Communications. (2015). About us. Retrieved 7 December 2015, from https://brasshorncommunications.uk/about/

Brennan, J. O., Hamre, J. J., & Lynn III, W. J. "Bill." (2015). Center for Strategic and International Studies Global Security Forum 2015: Opening Session. Retrieved 11 March 2016, from https://csis.org/files/attachments/151116_GSF_OpeningSession.pdf

Brown, I. (2011). Communications data retention in an evolving internet. *International Journal of Law and Information Technology*, 19(2), 95–109. https://doi.org/10.1093/ijlit/eaq016

Brown, I. (2014). The feasibility of transatlantic privacy-protective standards for surveillance. *International Journal of Law and Information Technology*, 23 (1), 1–18. https://doi.org/10.1093/ijlit/eau007

Brown, I., & Korff, D. (2009). Terrorism and the Proportionality of Internet Surveillance. *European Journal of Criminology*, 6 (2), 119–134. https://doi.org/10.1177/1477370808100541

Burns, D. (2015). Interview with Alison Macrina. Retrieved 8 November 2015, from http://hacklibraryschool.com/2015/05/27/interview-with-alison-macrina-flexlibris/

Cannataci, J. A. (2016). *Report of the Special Rapporteur on the right to privacy*. Retrieved 11 March 2016, from http://www.ohchr.org/Documents/Issues/Privacy/A-HRC-31-64.doc

Carmon, I. (2013). How we broke the NSA story. Retrieved 11 November 2015, from http://www.salon.com/2013/06/10/qa_with_laura_poitras_the_woman_behind_the_nsa_scoops/

Carpenter, Z. (2015). Librarians Versus the NSA. Retrieved 8 November 2015, from http://www.thenation.com/article/librarians-versus-nsa/

Casciani, D. (2003). Spy pictures of suffragettes revealed. Retrieved 8 November 2015, from http://news.bbc.co.uk/1/hi/magazine/3153024.stm

Castells, M. (2004). *The network society : a cross-cultural perspective*. Northampton, Mass.: Edward Elgar Publishing.

Charteris, S. (2009). *A local Inquiry into the Public Library Service Provided by Wirral Metropolitan Borough Council. Department for Culture, Media and Sport*. Retrieved 11 March 2016, from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/77448/wirral_local_inquiry.doc

Cilip. (2005). Statement on intellectual freedom, access to information and censorship. Retrieved 8 November 2015, from http://www.cilip.org.uk/cilip/archived-policy-statements/statement-intellectual-freedom-access-information-and-censorship

Cilip. (2012). Ethical Principles for Library and Information Professionals, 2004. Retrieved 11 March 2016, from http://www.cilip.org.uk/sites/default/files/documents/Ethical%20principles

%20for%20library%20and%20information%20professionals%20October%202012.pdf

Cilip. (2013). Short Briefing on the Public Libraries and Museums Act 1964, (January), 2013. Retrieved 11 March 2016, from http://www.cilip.org.uk/sites/default/files/documents/Briefing on Public Libraries and Museums Act 1964.pdf

Clark, I. (2012). *To what extent do community libraries address the concerns of the digital divide?* University of Aberystwyth.

Clark, I. (2016). Barclays and the library marketing opportunity. Retrieved 3 February 2016, from http://infoism.co.uk/2016/01/barclays-and-the-library-marketing-opportunity/

Cohen, J. E. (2013). What Privacy Is For. *Harvard Law Review*, 126 (7), 1904–1933. Retrieved 11 March 2016, from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2175406

Council of Europe. (2000). *New information technologies: public access and freedom of expression in cultural institutions*. Retrieved 11 March 2016, from http://www.coe.int/t/dg4/cultureheritage/culture/Resources/DECS_CULT_NTI_libex(2000)2_EN.pdf

Council of Europe. (2002). *Guidelines on human rights and the fight against terrorism*. Retrieved 11 March 2016, from http://www.coe.int/t/dlapil/cahdi/Source/Docs2002/H_2002_4E.pdf

Cox, J. (2015). Encryption App Telegram Probably Isn't as Secure for Terrorists as ISIS Thinks. Retrieved 20 November 2015, from http://motherboard.vice.com/read/encryption-app-telegram-probably-isnt-as-secure-for-terrorists-as-isis-thinks

Cox, J. (2016). Pssst, Your PGP Is Leaking. Retrieved 2 February 2016, from http://motherboard.vice.com/read/pssst-your-pgp-is-leaking

Crocker, A. (2015). EFF Asks Court on Behalf of Libraries and Booksellers to Recognize Readers' Right to Be Free of NSA's Online Surveillance. Retrieved 8 November 2015, from https://www.eff.org/deeplinks/2015/09/eff-asks-court-behalf-libraries-and-booksellers-recognize-readers-right-be-free

Crocker, A., Rumold, M., Greene, D., & Berlage, J. I. Wikimedia Foundation, et al. v. National Security Agency, et al., Case 1:15-cv-00662-TSE (2015). Retrieved 11 March 2016, from https://www.eff.org/files/2015/09/03/wikimedia_amicus_brief_filed.pdf

Cunningham, A. (2015). Android 6.0 re-implements mandatory storage encryption for new devices. Retrieved 24 February 2016, from http://arstechnica.com/gadgets/2015/10/android-6-0-re-implements-mandatory-device-encryption-for-new-devices/

De Marco, S., Robles, J. M., & Antino, M. (2014). Digital skills as a conditioning factor for digital political participation. *Communications*, 39 (1), 43–65. https://doi.org/10.1515/commun-2014-0004

Deloitte Insight. (2014). Data Nation 2014 Putting customers first. Retrieved 11 March 2016, from http://www2.deloitte.com/uk/en/pages/deloitte-analytics/articles/data-nation-2014-putting-

customers-first.html

DiMaggio, P., & Hargittai, E. (2001). From the 'Digital Divide' to 'Digital Inequality': Studying Internet Use as Penetration Increases. *Princeton Center for Arts and Cultural Policy Studies, Working Paper*, 15(15). Retrieved from http://webuse.umd.edu/webshop/resources/Dimaggio_Digital_Divide.pdf

Dobija, J. (2014). The First Amendment Needs New Clothes. *American Libraries*, 38 (8), 50–53.

Doyle-Burr, N. (2015). Despite Law Enforcement Concerns, Lebanon Board Will Reactivate Privacy Network Tor at Kilton Library. Retrieved 8 November 2015, from http://www.vnews.com/home/18620952-95/library-joins-privacy-network

Dredge, S. (2014). Worried about leaky chats? Messaging apps are responding with security features. Retrieved 17 January 2016, from http://www.theguardian.com/technology/2014/dec/11/messenger-private-chats

Dreyfuss, E. (2015). Sanity and Privacy Win Out in the Library-Tor Kerfuffle. Retrieved 8 November 2015, from http://www.wired.com/2015/09/sanity-privacy-win-library-tor-kerfuffle/

Eubanks, V. (2011). Digital dead end fighting for social justice in the information age. Cambridge, Mass.: MIT Press.

European Court of Human Rights. (1998). Osman v. The United Kingdom. Retrieved 11 March 2016, from http://hudoc.echr.coe.int/eng?i=001-58257

European Court of Human Rights. (2000). Case of Amann v. Switzerland, (September 2000). Retrieved 11 March 2016, from http://hudoc.echr.coe.int/eng?i=001-58497

European Court of Human Rights. (2008). S. and Marper v. The United Kingdom. Retrieved 11 March 2016, from http://hudoc.echr.coe.int/eng?i=001-90051

European Court of Human Rights. (2015). Roman Zakharov v. Russia. Retrieved 11 March 2016, from http://hudoc.echr.coe.int/fre?i=001-159324

European Court of Justice. (2015). Maximillian Schrems v. Data Protection Commissioner. Retrieved 8 November 2015, from http://curia.europa.eu/juris/document/document.jsf?text=&docid=168421&pageIndex=0&doclang=en

Evans, M. (2005). The data-informed marketing model and its social responsibility. In S. Lace (Ed.), *The glass consumer life in a surveillance society*. Bristol: Policy.

Evans, R., & Lewis, P. (2013). *Undercover : the true story of Britain's secret police*. London: Faber and Faber.

Farivar, C. (2012). Private: some search engines make money by not tracking users. Retrieved 16 February 2016, from http://arstechnica.com/business/2012/05/private-the-search-engines-that-make-money-by-not-tracking-users/

Flashpoint Partners. (2014). *Measuring the Impact of the Snowden Leaks on the Use of Encryption by*

Online Jihadists. Retrieved 11 March 2016, from https://fpjintel.com/portal/assets/File/Flashpoint_Jihadi_Encryption_Software_Sept2014.pdf

Foucault, M. (1977). *Discipline and punish : the birth of the prison*. New York: Pantheon Books.

Fuchs, C. (2010). *Internet and society: social theory in the information age*. London: Routledge.

Gallagher, R. (2015). From Radio to Porn, British Spies Track Web Users' Online Identities. Retrieved 8 November 2015, from https://theintercept.com/2015/09/25/gchq-radio-porn-spies-track-web-users-online-identities/

Gangadharan, S. P. (2012). Digital inclusion and data profiling. *First Monday*. https://dx.doi.org/10.5210/fm.v17i5.3821

Gibbs, S. (2015a). Facebook accused of spying on Belgian citizens like the NSA. Retrieved 8 November 2015, from http://www.theguardian.com/technology/2015/sep/21/facebook-spying-belgian-citizens-nsa-data-regulator-lawsuit

Gibbs, S. (2015b). Google can unlock some Android devices remotely, district attorney says. Retrieved 6 December 2015, from http://www.theguardian.com/technology/2015/nov/24/google-can-unlock-android-devices-remotely-if-phone-unencrypted

Giroux, H. A. (2015). Totalitarian Paranoia in the Post-Orwellian Surveillance State. *Cultural Studies*, 29 (2), 108–140. https://doi.org/10.1080/09502386.2014.917118

Google. (2015). Ads in Gmail. Retrieved 8 November 2015, from https://support.google.com/mail/answer/6603

Greenwald, G., MacAskill, E., Poitras, L., Ackerman, S., & Rushe, D. (2013). Microsoft handed the NSA access to encrypted messages. Retrieved 8 November 2015, from http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data

grugq. (2015a). Operational Telegram. Retrieved 20 November 2015, from http://grugq.tumblr.com/post/133453305233/operational-telegram

grugq. (2015b). Signals, Intelligence. Retrieved 20 November 2015, from https://medium.com/@thegrugq/signal-intelligence-free-for-all-5993c2f72f90#.kcrudz6bm

Hargittai, E. (2002). Second-Level Digital Divide: Differences in people's online skills. *First Monday*. Retrieved 11 March 2016, from http://firstmonday.org/ojs/index.php/fm/article/view/942/864

Harris, J. (2009). Wirral library closures: Centralisation is undone by people power. Retrieved 28 January 2016, from http://www.theguardian.com/commentisfree/2009/apr/06/libraries-andyburnham

Home Office. (2012). *Draft Communications Data Bill*. Retrieved 11 March 2016, from http://www.official-documents.gov.uk/document/cm83/8359/8359.pdf

Home Office. (2015). *Draft Investigatory Powers Bill*. Retrieved 11 March 2016, from

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf

Home Office. (2016a). *Investigatory Powers Bill : Government Response to Pre-Legislative Scrutiny*. Retrieved 11 March 2016, from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504174/54575_Cm_9219_WEB.PDF

Home Office. (2016b). *Investigatory Powers Bill: overarching documents – Publications – GOV.UK*. Retrieved 11 March 2016, from https://www.gov.uk/government/publications/investigatory-powers-bill-overarching-documents

Humphreys, L. (2011). Who's Watching Whom? A Study of Interactive Technology and Surveillance. *Journal of Communication*, 61 (4), 575–595. https://doi.org/10.1111/j.1460-2466.2011.01570.x

Ifla. (2015). IFLA Publishes a Statement on Privacy in the Library Environment. Retrieved 8 November 2015, from http://www.ifla.org/node/9803

Ipsos MORI. (2015). *Basic Digital Skills*. Retrieved 11 March 2016, from https://goon-uk-prod.s3-eu-west-1.amazonaws.com/uploads/Basic Digital Skills_UK Report 2015_131015_FINAL.pdf

Jordan, T. (2015). *Information politics: liberation and exploitation in the digital society*. Pluto Press.

Kaye, D. (2015). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. Retrieved 11 March 2016, from http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx

King, S., McMenemy, D., & Poulter, A. (2006). Effectiveness of ICT training for public library staff in the UK: staff views. *The Electronic Library*, 24 (2), 265–276. https://doi.org/10.1108/02640470610649281

Lee, M. (2015a). Chatting in Secret While We're All Being Watched. Retrieved 5 March 2016, from https://theintercept.com/2015/07/14/communicating-secret-watched/

Lee, M. (2015b). Edward Snowden Explains How To Reclaim Your Privacy. Retrieved 16 February 2016, from https://theintercept.com/2015/11/12/edward-snowden-explains-how-to-reclaim-your-privacy/

Leopold, J. (2014). Exclusive: Emails reveal close Google relationship with NSA. Retrieved 8 November 2015, from http://america.aljazeera.com/articles/2014/5/6/nsa-chief-google.html

Lichtblau, E. (2005). F.B.I., Using Patriot Act, Demands Library's Records. Retrieved 24 February 2016, from http://www.nytimes.com/2005/08/26/politics/fbi-using-patriot-act-demands-librarys-records.html

Lynch, M. P. (2015). The philosophy of privacy: why surveillance reduces us to objects. Retrieved 23 February 2016, from http://www.theguardian.com/technology/2015/may/07/surveillance-privacy-philosophy-data-internet-things

Lyon, D. (1994). From Big Brother to Electronic Panopticon. In *The Electronic Eye: The Rise of Surveillance Society* (pp. 57–80). Retrieved 11 March 2016, from http://home.fnal.gov/~annis/digirati/otherVoices/Lyon.html

Lyon, D. (2007). *Surveillance studies: an overview*. Cambridge, UK; Malden, MA: Polity.

Lyon, D. (2010). Liquid Surveillance: The Contribution of Zygmunt Bauman to Surveillance Studies. *International Political Sociology*, 4 (4), 325–338. https://doi.org/10.1111/j.1749-5687.2010.00109.x

Lyon, D. (2015). The Snowden Stakes: Challenges for Understanding. *Surveillance and Society*, 13 (2), 139–152.

Maass, P. (2013). How Laura Poitras Helped Snowden Spill His Secrets. Retrieved 23 February 2016, from http://www.nytimes.com/2013/08/18/magazine/laura-poitras-snowden.html

MacAskill, E. (2013). NSA paid millions to cover Prism compliance costs for tech companies. Retrieved 11 November 2015, from http://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid

MacAskill, E., Borger, J., Hopkins, N., Davies, N., & Ball, J. (2013). GCHQ taps fibre-optic cables for secret access to world's communications. Retrieved 12 November 2015, from http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

Macrina, A. (2015). Accidental Technologist: The Tor Browser and Intellectual Freedom in the Digital Age. *Reference and User Services Quarterly*, 54 (4), 17–21. http://dx.doi.org/10.5860/rusq.54n4.17

Macrina, A., & Fatemi, N. (2015). Tor exit relays in libraries: a new LFP project. Retrieved 8 November 2015, from https://libraryfreedomproject.org/torexitpilotphase1/

Mason, R. (2015). UK spy agencies need more powers, says Cameron. Retrieved 12 November 2015, from http://www.theguardian.com/uk-news/2015/jan/12/uk-spy-agencies-need-more-powers-says-cameron-paris-attacks

McGarr, S. (2015). EU Law Analysis: Do Facebook and the USA violate EU data protection law? The CJEU hearing in Schrems. Retrieved 8 November 2015, from http://eulawanalysis.blogspot.co.uk/2015/03/does-facebook-and-usa-violate-eu-data.html

McLaughlin, J. (2015). Scope of Secretive FBI National Security Letters Revealed by First Lifted Gag Order. Retrieved 2 December 2015, from https://theintercept.com/2015/11/30/scope-of-secretive-fbi-national-security-letters-revealed-by-first-lifted-gag-order/

Mervyn, K., Simon, A., & Allen, D. K. (2014). Digital inclusion and social inclusion: a tale of two cities. *Information, Communication & Society*, 17 (9), 1086–1104. https://doi.org/10.1080/1369118X.2013.877952

Min, S.-J. (2010). From the digital divide to the democratic divide: internet skills, political interest, and the second-level digital divide in political internet use. *Journal of Information Technology*

& Politics, 7, 22–35. https://doi.org/10.1080/19331680903109402

Moody, G. (2016). It's legal for GCHQ to break into computers and install spyware, tribunal rules. Retrieved 16 February 2016, from http://arstechnica.co.uk/tech-policy/2016/02/its-legal-for-gchq-to-break-into-computers-and-install-spyware-tribunal-rules/

Morris, D. S., & Morris, J. S. (2013). Digital inequality and participation in the political process: Real or imagined? *Social Science Computer Review*, 31 (5), 589–600. https://doi.org/10.1177/0894439313489259

Nakashima, E., & Peterson, A. (2016). The British want to come to America — with wiretap orders and search warrants. Retrieved 16 February 2016, from https://www.washingtonpost.com/world/national-security/the-british-want-to-come-to-america--with-wiretap-orders-and-search-warrants/2016/02/04/b351ce9e-ca86-11e5-a7b2-5a2f824b02c9_story.html

Norcie, G., Blythe, J., Caine, K., & Camp, L. J. (2014). Why Johnny Can't Blow the Whistle: Identifying and Reducing Usability Issues in Anonymity Systems. *Proceedings 2014 Workshop on Usable Security*. https://doi.org/10.14722/usec.2014.23022

O'Neill, P. H. (2016). New Hampshire bill allows public libraries to run Tor in the face of federal challenges. Retrieved 24 February 2016, from http://www.dailydot.com/politics/new-hampshire-tor-library-legislation/

Ofcom. (2015). *Adults' media use and attitudes report*. Retrieved from http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/media-lit-10years/2015_Adults_media_use_and_attitudes_report.pdf

Office for National Statistics. (2015). *Internet Access – Households and Individuals 2015*. Retrieved from http://www.ons.gov.uk/ons/rel/rdit2/internet-access---households-and-individuals/2015/stb-ia-2015.html

Olsen, M., Schneier, B., Zittrain, J., Gasser, U., Olsen, M. G., Gertner, N., O'Brien, D. R. (2016). *Don't Panic. Making Progress on the "Going Dark" Debate.* The Berkman Center for Internet & Society at Harvard University. https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf

Park, Y. J. (2013). Offline Status, Online Status: Reproduction of Social Categories in Personal Information Skill and Knowledge. *Social Science Computer Review*, 31 (6), 680–702. https://doi.org/10.1177/0894439313485202

Park, Y. J. (2014). My whole world's in my palm! The second-level divide of teenagers' mobile use and skill. *New Media & Society*, 17 (6), 977–995. https://doi.org/10.1177/1461444813520302

Peers, S. (2015). American Mass Surveillance of EU citizens: Is the End Nigh? Retrieved 8 November 2015, from http://eulawanalysis.blogspot.be/2015/09/american-mass-surveillance-of-eu.html

Pew Research Center. (2014). Global Opinions of U.S. Surveillance: United Kingdom. Retrieved 16

February 2016, from http://www.pewglobal.org/2014/07/14/nsa-opinion/country/united-kingdom/

President's Commission on Law Enforcement and Administration of Justice. (1967). The Challenge of Crime in a Free Society, (February), 1–342. Retrieved from https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=42

Price, D. (2013). A Social History of Wiretaps. Retrieved 27 November 2015, from http://www.counterpunch.org/2013/08/09/a-social-history-of-wiretaps-2/

Price, R. (2015). Android phones are cheaper than ever because of "growing income inequality" — and that's a good thing. Retrieved 8 November 2015, from http://uk.businessinsider.com/android-iphone-price-disparity-increase-2015-2

Reiman, P. (1996). Cryptography and the First Amendment: The Right to be Unheard. *John Marshall Journal of Computer & Information Law*, 14 (2), 1–29. http://repository.jmls.edu/cgi/viewcontent.cgi?article=1313&context=jitpl

Renaud, K., Volkamer, M., & Renkema-Padmos, A. (2014). Why doesn't Jane protect her privacy? *Lecture Notes in Computer Science (including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8555 LNCS, 244–262. https://doi.org/10.1007/978-3-319-08506-7_13

Richards, N. M. (2008). Intellectual Privacy. *Texas Law Review*, 87, 387. https://doi.org/10.2139/ssrn.1108268

Richards, N. M. (2013). The dangers of surveillance. *Harvard Law Review*, 126 (7), 1934–1965. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2239412

Rogaway, P. (2015). The Moral Character of Cryptographic Work. Retrieved from http://web.cs.ucdavis.edu/~rogaway/papers/moral-fn.pdf

Ruoti, S., Andersen, J., Zappala, D., & Seamons, K. (2015). Why Johnny Still, Still Can't Encrypt: Evaluating the Usability of a Modern PGP Client. *ArXiv E-Prints*. Retrieved from http://arxiv.org/abs/1510.08555

Rushe, D. (2014). Yahoo $250,000 daily fine over NSA data refusal was set to double "every week." Retrieved 8 November 2015, from http://www.theguardian.com/world/2014/sep/11/yahoo-nsa-lawsuit-documents-fine-user-data-refusal

Schell, J. (2013). America's Surveillance Net. Retrieved 8 November 2015, from http://www.thenation.com/article/americas-surveillance-net/

Schriner, J. (2015). Radical Librarian-Technologists. *Journal of Radical Librarianship*. Retrieved from https://journal.radicallibrarianship.org/index.php/journal/article/view/6/14

Shalal, A. (2016). Former Google CEO Schmidt to head new Pentagon innovation board. Retrieved 6 March 2016, from http://www.reuters.com/article/us-usa-military-innovation-idUSKCN0W421V

Shema, M. (2011). Web Security: Why You Should Always Use HTTPS. Retrieved 16 February 2016, from http://mashable.com/2011/05/31/https-web-security/

Simonite, T. (2015). Is Google's Lackluster Support for Encryption a Human Rights Issue? Retrieved 11 November 2015, from http://www.technologyreview.com/news/543161/why-google-trailing-apple-on-encryption-support-is-a-human-rights-issue/

Sinclair Brody, S. (2016). Protecting Data Privacy With User-Friendly Software – Council on Foreign Relations. Retrieved 23 February 2016, from http://www.cfr.org/privacy/protecting-data-privacy-user-friendly-software/p37551

Smith, D., & Chamberlain, P. (2015). *Blacklisted: the secret war between big business and union activists*. Oxford: New Internationalist Publications Ltd.

Spacey, R. E. (2003). An Evaluation of the New Opportunities Fund ICT Training Programme for Public Library Staff, UK. In *World Library and Information Congress : 69th IFLA General Conference and Council* (pp. 1–21). Retrieved from http://archive.ifla.org/IV/Ifla69/papers/004e-Spacey.pdf

Sparks, C. (2013). What is the "digital divide" and why is it important? *Javnost*, 20 (2), 27–46. https://doi.org/10.1080/13183222.2013.11009113

St Vincent, S. (2016). Did the European Court of Human Rights Just Outlaw "Massive Monitoring of Communications" in Europe? Retrieved 21 January 2016, from https://cdt.org/blog/did-the-european-court-of-human-rights-just-outlaw-massive-monitoring-of-communications-in-europe/

Telegram. (2014). $300,000 for Cracking Telegram Encryption. Retrieved 24 November 2015, from https://telegram.org/blog/cryptocontest

Temperton, J. (2015a). AVG can sell your browsing and search history to advertisers. Retrieved 8 November 2015, from http://www.wired.co.uk/news/archive/2015-09/17/avg-privacy-policy-browser-search-data

Temperton, J. (2015b). Lords attempt to sneak through snoopers' charter again. Retrieved 11 November 2015, from http://www.wired.co.uk/news/archive/2015-02/02/snoopers-charter-again

Temperton, J. (2015c). No U-turn: David Cameron still wants to break encryption. Retrieved 11 November 2015, from http://www.wired.co.uk/news/archive/2015-07/15/cameron-ban-encryption-u-turn

The Investigatory Powers Tribunal. Liberty v GCHQ & Othrs (2015). Retrieved from http://www.ipt-uk.com/docs/Liberty-Order6Feb15.pdf

The Investigatory Powers Tribunal. Lucas & Othrs v Security Service & Othrs (2015). Retrieved from http://www.intelligencecommissioner.com/docs/Caroline_Lucas_JUDGMENT.pdf

The Investigatory Powers Tribunal. Privacy International & Othrs v GCHQ & Othrs (2016).

Retrieved from http://www.ipt-uk.com/docs/Privacy_Greennet_and_Sec_of_State.pdf

Tor Metrics. (2015). Direct users by country. Retrieved 2 December 2015, from https://metrics.torproject.org/userstats-relay-country.html

Travis, A. (2016). Snooper's charter: cafes and libraries face having to store Wi-Fi users' data. Retrieved 18 February 2016, from http://www.theguardian.com/world/2016/jan/13/snoopers-charter-theresa-may-cafes-wifi-network-store-customers-data

Vagle, J. L. (2015). Furtive Encryption: Power, Trust, and the Constitutional Cost of Collective Surveillance. *Indiana Law Journal*, 90 (101). Retrieved 12 March 2016, from http://ilj.law.indiana.edu/articles/11-Vagle.pdf

Vickery, J. R. (2014). 'I don't have anything to hide, but … ': the challenges and negotiations of social and mobile media privacy for non-dominant youth. *Information, Communication & Society*, 18 (3), 281–294. https://doi.org/10.1080/1369118X.2014.989251

Whitten, A., & Tygar, J. D. (1999). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. *Proceedings of the 8th USENIX Security Symposium*, 169–184. Retrieved from https://www.usenix.org/legacy/events/sec99/full_papers/whitten/whitten_html/index.html

Wolf, N. (2012). The new totalitarianism of surveillance technology. Retrieved 8 November 2015, from http://www.theguardian.com/commentisfree/2012/aug/15/new-totalitarianism-surveillance-technology

YouGov. (2015). *YouGov / Sunday Times Survey Results*. Retrieved from https://d25d2506sfb94s.cloudfront.net/cumulus_uploads/document/wt26kxdn72/YG-Archive-Pol-Sunday-Times-results-160115.pdf

Zdziarski, J. (2014). Identifying back doors, attack points, and surveillance mechanisms in iOS devices. *Digital Investigation*, 11 (1), 3–19. https://doi.org/10.1016/j.diin.2014.01.001